IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

ALLIANCE FOR AUTOMOTIVE INNOVATION Plaintiff, vs. MAURA HEALEY, ATTORNEY GENERAL OF THE COMMONWEALTH OF MASSACHUSETTS in her official capacity, Defendant.	C.A. No. 1:20-cv-12090-DPW

PLAINTIFF'S OPPOSITION TO MOTION TO DISMISS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Federal Constitutional Provisions, Statutes, and Regulations

State Statutes and Legislation

Other Authorities

INTRODUCTION

The Attorney General's Motion to Dismiss ("Mot.") disregards the well-pled allegations of the Complaint of Plaintiff Alliance for Automotive Innovation ("Plaintiff" or "Auto Innovators"). Further, the Attorney General repeatedly downplays the effects of Massachusetts SD645 (the "Data Law")—a first-of-its-kind law that in the course of promoting wide-ranging open access to vehicle data would eliminate auto manufacturers' ability to control access to their electronic vehicle systems and keep cyberhackers or other unauthorized users out. As the Complaint alleges and Plaintiff will demonstrate at trial, the Data Law conflicts with the requirements, purposes, and objectives of several federal laws—most notably the National Traffic and Motor Vehicle Safety Act, 49 U.S.C. § 30101, *et seq.* ("Vehicle Safety Act") and the Clean Air Act, 42 U.S.C. § 7401, *et seq.*—and it is not possible for the manufacturers to both comply with the new Data Law and those preexisting federal statutes. The remaining counts in the Complaint should be stayed pending trial on the merits of the Vehicle Safety Act and Clean Air Act claims, though each count plausibly states a claim for relief. Finally, Plaintiff has more than satisfied the standards for associational standing to assert claims on behalf of its many auto manufacturer members, all of whom are aligned on these claims.

BACKGROUND

The Data Law upends the current federal regulatory regime around vehicle safety.[1] Section 2 immediately eliminates manufacturers' ability to have any involvement in the control of access to their vehicle systems by mandating that "on-board diagnostic systems" in any vehicles "sold in the Commonwealth" be "standardized and not require any authorization by the manufacturer, directly or indirectly," unless a standardized authorization system is used across all makes and

[1] A copy of the Data Law can be found at ECF 28-1.

models and administered by a third party,—a system that does not exist today. Compl. ¶ 9. Section 3 requires that, for all vehicles from Model Year 2022 onward (*i,e.*, immediately), manufacturers must install an open-access, bi-directional "platform" to allow third parties unfettered access to use, modify, or write "any vehicle-specific data, including telematics system data, generated, stored in or transmitted by a motor vehicle used for or otherwise related to the diagnosis, repair or maintenance of the vehicle" to the platform. Compl. ¶¶ 20-22, 39.

As alleged in the Complaint, it is impossible for auto manufacturers to comply with the requirements of the Data Law without eliminating important cybersecurity controls to firmware that operates safety-critical systems, including steering, acceleration, and braking, as well as emissions, in direct contravention of important vehicle safety objectives articulated by the expert federal agency. Compl. ¶¶ 42-43, 56-58, 97, 105-106. The National Highway Traffic Safety Administration ("NHTSA")—the agency charged with enforcement of the federal Vehicle Safety Act—has noted that manufacturers have designed these cybersecurity controls in accordance with the Vehicle Safety Act, and the Data Law would require manufacturers to render those important safety features inoperative in order to satisfy the open access requirements of the statute. Compl. Ex. A, at 3-4. Because the elimination of those cybersecurity controls is inconsistent with the clear objectives of the Vehicle Safety Act and, with respect to emissions, the Clean Air Act, and would subject the manufacturers to potential liability for violation of those federal statutes, the Data Law is preempted under the Supremacy Clause of the United States Constitution.

ARGUMENT

On a motion to dismiss pursuant to Rule 12(b)(6), the court "must accept the allegations of the complaint as true, drawing all reasonable inferences in favor of the plaintiff." *Alicea v. LT's Benjamin Records*, 762 F. Supp. 2d 299, 302 (D. Mass. 2011). A complaint that states a plausible

claim for relief on its face must survive a motion to dismiss. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). Likewise, on a motion to dismiss under Rule 12(b)(1), the court must "credit the plaintiff's well-pled factual allegations and draw all reasonable inferences in the plaintiff's favor." *Sanchez ex rel. D.R.-S. v. United States*, 671 F.3d 86, 92 (1st Cir. 2012).

I. Plaintiff Has Stated a Plausible Preemption Claim Under the Vehicle Safety Act and Vehicle Safety Standards.

The Data Law is preempted under the Vehicle Safety Act and related federal motor vehicle safety standards for two independent reasons.

First, the Data Law requires auto manufacturers to eliminate existing cybersecurity controls that protect core vehicle functions and thereby ensure the safe operation of vehicles. Compl. ¶¶ 58, 71, 105. Under well-settled preemption principles, that state-law obligation conflicts with the purposes and objectives of the Vehicle Safety Act, and the obligations of auto manufacturers under that Act. NHTSA—the agency charged with enforcement of the Act—has made clear, time and again, including with respect to the Data Law itself, that manufacturers have a federal safety obligation to protect their vehicles against cybersecurity threats and, if they are not successful at doing so, federal law requires them to conduct safety recalls to remedy the deficiency. *Id.* ¶¶ 3, 68-69, 101-106.

Second, the Vehicle Safety Act explicitly prohibits an automaker from "mak[ing] inoperative any . . . element of design installed on or in a motor vehicle . . . in compliance with an applicable motor vehicle safety standard." 49 U.S.C. § 30122(b). Automakers have included cybersecurity access controls in the systems they install in compliance with several safety standards, Compl. ¶ 106, which access controls would need to be removed to comply with the Data Law, *id.* ¶¶ 58, 71, 106. The removal of those important cybersecurity controls would violate the Vehicle Safety Act. *Id.* ¶ 106.

A. The Data Law Conflicts with the Objectives of the Vehicle Safety Act.

The Attorney General posits an alternative reality where conflict preemption takes on the requirements of express preemption. *See* Mot. 1-6, 9-10. As this Court has recognized, "conflict preemption" differs from "express preemption." Express preemption requires statutory language revealing an "explicit congressional intent to preempt state law." In contrast, conflict preemption, on which Plaintiff bases its claims here, occurs when "compliance with both state and federal law is impossible, or when the state law stands as an obstacle to the accomplishment of the full purposes and objectives of Congress." *Town of Acton v. W.R. Grace & Co.*, No. 13–12376–DPW, 2014 WL 7721850, at *9 (D. Mass. Sept. 22, 2014) (quoting *Weaver's Cove Energy, LLC v. R.I. Coastal Res. Mgmt. Council*, 589 F.3d 458, 472 (1st Cir. 2009)).

Plaintiff's claim fits neatly within the conflict-preemption framework that the Supreme Court articulated in *Geier v. American Honda Motor Co., Inc.*, 529 U.S. 861, 870 (2000).[2] The *Geier* standard looks to whether, "'under the circumstances of th[e] particular case," the state law "stands as an obstacle to the accomplishment and execution of the full *purposes and objectives* of Congress'—whether that 'obstacle' goes by the name of 'conflicting; contrary to; . . . repugnance; difference; irreconcilability; inconsistency; violation; curtailment; . . . interference,' or the like." 529 U.S. at 873 (quoting *Hines v. Davidowitz*, 312 U.S. 52, 67 (1941)) (emphasis added). The analysis extends beyond statutory language to the federal law's "purpose and intended effects." *Comm'ns Imp. Exp. S.A. v. Rep. of the Congo*, 757 F.3d 321, 326 (D.C. Cir. 2014) (internal

[2] *Geier* involved a provision in an earlier version of Federal Motor Vehicle Safety Standard 208 that required auto manufacturers to install passive restraints in cars, but did not specify whether to use airbags, automatic seatbelts, or some other passive system. 529 U.S. at 865-68. The Court held that the standard preempted a state tort suit against Honda for failing to install a driver's side airbag that might have protected Geier from severe injuries sustained in a crash. *Id.* at 874-75. The state law stood as an obstacle to the accomplishment and execution" of an important "federal objective[]"—namely, giving manufacturers a choice among different kinds of passive restraint systems. *Id.* at 881, 83.

citations omitted). As a result, "federal law may preempt state law even if the conflict between the two is not facially apparent—as when, for example, the federal and state laws govern different subject matters." *Id.* The critical question is whether the state law serves "as an obstacle to the accomplishment and execution" of important "federal objectives." *Geier*, 529 U.S. at 881.

The Vehicle Safety Act confers twin authorities upon NHTSA for the purpose of protecting the safety of motor vehicles. One is the authority to issue and enforce Federal Motor Vehicle Safety Standards ("FMVSS") for new vehicles and equipment under Section 30111 of the Act. FMVSS issued under that section expressly preempt inconsistent state or local laws, pursuant to Section 30303(b) of the Act. The statute also directs NHTSA to require manufacturers to conduct notification and remedy campaigns ("recalls") to address and remediate safety-related defects arising in vehicles in the field, pursuant to Sections 30118-30120 of the Act. The Act requires manufacturers to initiate recalls when safety defects are identified, and also authorizes NHTSA to order a recall if the manufacture does not commence one. As NHTSA recently noted:

> The Safety Act defines ''motor vehicle safety" as "the performance of a motor vehicle or motor vehicle equipment in a way that protects the public against unreasonable risk of accidents occurring because of the design, construction, or performance of a motor vehicle, and against unreasonable risk of death or injury in an accident, and includes nonoperational safety of a motor vehicle." This common term, which is the driving force behind both FMVSS-setting and defect determinations, ***acts to link NHTSA's execution of its authorities against unreasonable safety risks inherently***, both in setting FMVSS and in overseeing the safety of vehicle design, construction, and performance.

85 Fed. Reg. 83143, 83150 (Dec. 21, 2020) (footnote omitted) (emphasis added).

Over the fifty-plus years of NHTSA's history, it has rarely had to order a recall. More than ten thousand voluntary recalls[3] have been conducted over the years, because NHTSA has been

[3] To be clear, "voluntary" recalls are not optional. They are required by the Vehicle Safety Act when a vehicle contains a defect related to motor vehicle safety. *See* 49 U.S.C. §§ 30118–30120. In common usage, the term "voluntary recall" means a recall that the manufacturer initiated on its own to comply with the statute without awaiting an Order from NHTSA.

transparent with the industry about NHTSA's interpretation of the term "defect related to motor vehicle safety," the statutory trigger for a recall. If NHTSA reasonably concludes that a particular condition is a "defect related to motor vehicle safety," federal law requires the manufacturer to conduct a recall to fix the condition.

NHTSA communicates its interpretation of the term "defect related to motor vehicle safety" to manufacturers in several ways. It conducts defect investigations in public, to create transparency regarding the conditions that NHTSA is evaluating as potential safety-related defects and to the resolution of those investigations. Sometimes the investigations result in a recall because NHTSA concludes that the condition is a safety-related defect, and the manufacturer elects not to challenge that conclusion. After the recall is announced and the closing report is published, the entire industry is on notice of NHTSA's conclusion.

NHTSA is also required by the Vehicle Safety Act to consider petitions from the public for a finding that a particular condition is a safety-related defect. *See* 49 U.S.C. § 30162. NHTSA responds to these petitions with either a grant or a denial. A decision to grant results in further investigation, which will eventually be closed with a public report whether the investigation results in a recall or not. A denial results in a Federal Register notice explaining why NHTSA was not likely to find the condition to be a safety-related defect. Either way, the industry is educated as to NHTSA's interpretation of the term "defect related to motor vehicle safety."

NHTSA also occasionally publishes guidance for the regulated industry on its interpretation of the term "defect related to motor vehicle safety" as it applies in particular contexts or to particular conditions. For example, a few years ago NHTSA issued guidance confirming that, if an aftermarket software update creates or introduces an unreasonable safety risk to motor vehicle systems, "then that safety risk constitutes a defect compelling a recall." 81 Fed. Reg.

65705, 65709 (Sept. 23, 2016). When NHTSA publishes such guidance, it does so to assist the industry in complying with its statutory obligation to conduct recalls when safety defects arise. Such guidance is especially useful for understanding NHTSA's view of emerging hazards.

In this case, Plaintiff's Complaint cites to the cybersecurity guidance as providing NHTSA's interpretation of when a cybersecurity vulnerability rises to a safety-related defect requiring a recall. If NHTSA requires a recall under the Vehicle Safety Act for any reason, a state is preempted from requiring the manufacturer to create or maintain the vehicle condition giving rise to the recall, as it would be impossible to satisfy both the Vehicle Safety Act and the state law.

The Attorney General argues that NHTSA's cybersecurity guidance is irrelevant for preemption purposes. *See* Mot. 6-7. But when adjudicating conflict preemption, courts routinely look to agency expressions of policy to determine the content and scope of the federal policy at issue and, ultimately, whether a conflict with the purposes and objectives of federal statute exists.[4] An "agency's own views should make a difference" in determining preemption because the agency is "likely to have a thorough understanding of its own regulation and its objectives and is uniquely qualified to comprehend the likely impact of state requirements." *Geier*, 529 U.S. at 883.

The conflict here is between the Vehicle Safety Act's requirements to recall vehicles containing safety-related defects and the Data Law's requirement that manufacturers remove important cybersecurity controls. *E.g.*, Compl. ¶¶ 99-105. While NHTSA's guidance has left

[4] *See, e.g., Altra Grp., Inc. v. Good*, 555 U.S. 70, 89 (2008) (considering FTC policy guidance but after review of it concluding that "the FTC has no longstanding policy authorizing collateral representations"); *Charter Advanced Servs. (MN), LLC v. Lange*, 903 F.3d 715, 718 (8th Cir. 2018) (holding that FCC's policy of nonregulation regarding "information service" under the Telecommunications Act preempted state law because "any state regulation of an information service conflicts with the federal policy of nonregulation so that such regulation is preempted by federal law") (internal citations omitted); *Computer and Commc'ns Indus. Ass'n v. FCC*, 693 F.2d 198, 214-18 (D.C. Cir. 1982) (holding that a federal agency may preempt a state regulation to promote a federal policy of fostering competition in the market for customer premises equipment, despite lack of explicit regulatory language).

manufacturers flexibility concerning how to safeguard safety-critical vehicle systems, the agency has stated in no uncertain terms that those systems must be protected in ways that are antithetical to the requirements of the Data Law—*e.g.*, through manufacturers controlling access to firmware that executes core vehicle functions like acceleration, braking, and steering; isolating vehicle systems from one another; and maintaining non-standardized approaches across the industry to prevent large-scale hacking. Compl. Ex. A, at 3-4. NHTSA has made clear that (a) failure to maintain adequate controls would give rise to a safety-related defect and hence recall obligations under the Vehicle Safety Act and (b) the Data Law's requirements cannot be satisfied by manufacturers without removing current controls. *See id.* at 3. The actual conflict giving rise to preemption, then, is with the Vehicle Safety Act's requirements themselves, and not the guidance.

Nor is this conflict theoretical. NHTSA has enforced the obligation to include cybersecurity protections in vehicle systems that control core vehicle functions. In 2015, NHTSA found that some Chrysler vehicles had a flaw in their radio software security that "could allow unauthorized third-party access to some networked vehicle control systems." ECF 28-5. Specifically, NHTSA determined that third-party "[e]xploitation of the software security vulnerabilities could lead to exposing the driver, the vehicle occupants or any other individual or vehicle with proximity to the affected vehicle to a potential risk of injury." *Id.* Ultimately, Chrysler worked with NHTSA to issue a voluntary recall of 1,410,000 vehicles to repair the software vulnerability and avoid a finding of a statutory violation. Compl. ¶ 73.

As the Chrysler recall illustrates, any manufacturer who runs afoul of federal policy requiring strong cybersecurity protections by not maintaining robust access controls around vehicle systems—as the Complaint plausibly alleges Plaintiff's members cannot do while simultaneously complying with the Data Law's open access requirements and timeline, *see* Compl.

¶¶ 51-52, 57-58, 71—would face consequences under the federal Vehicle Safety Act that would conflict with their obligations under the new Massachusetts law.

The Attorney General suggests that implied preemption law has changed significantly since *Geier*. *See* Mot. 4-6, 10-11. But the cases on which it relies are far afield and, in any event, do not scuttle longstanding principles of conflict preemption. In *Virginia Uranium, Inc. v. Warren* (cited at Mot. 4, 10, 11), for instance, a plaintiff mining company alleged that a Virginia law preventing state agencies from accepting uranium mining permit applications was preempted by the Atomic Energy Act. 139 S. Ct. 1894, 1898 (2019) (lead op. of Gorsuch, J.) There, the federal agency charged with implementing the Act had "long believed, and still maintain[ed] that the [statute] afford[ed] it no authority to regulate uranium mining on private land"—the very matter at issue in the preemption case. *Id.* at 1903. In those circumstances—inapplicable here—the Supreme Court said that it would not try to "discern what motivates legislators individually and collectively" to try to give effect to "abstract and unenacted legislative desires" about matters not regulated. *Id.* at 1907.[5]

The Attorney General's other recent authority—*Kansas v. Garcia*, 140 S. Ct. 791 (2020) (cited at Mot. 5, 6, 10)—involved an allegation that state identify-theft and false-information statutes were preempted by the federal Immigration Reform and Control Act. *Id.* at 794-95. Unsurprisingly, the Supreme Court held that there is "no basis for inferring that federal criminal statutes preempt state laws whenever they overlap," adding that "[o]ur federal system would be turned upside down if we were to hold that federal criminal law preempts state law whenever they

[5] The Court added that its prior precedent allowed the inference of "congressional intent to displace a state law that makes compliance with a federal statute impossible." *Va. Uranimum*, 139 S. Ct. at 1908 (citing *English v. Gen. Elec. Co.*, 496 U.S. 72, 79 (1990)). But, unlike here, the *Virginia Uranium* plaintiff did not "pursu[e] an argument along any of these lines and understandably so," since, unlike here, it could "comply with both state and federal laws." *Id.*

overlap." *Id.* at 806. Here, by contrast, the Complaint alleges something much more than a mere overlap in statutory regimes; rather, the Complaint alleges that the Data Law impermissibly puts Plaintiff's members in the position of being forced to choose between compliance with two conflicting regulatory regimes, as full compliance with both the new Data Law and the Vehicle Safety Act is not possible.

The Attorney General's repeated reliance on *Capron v. Office of Attorney General of Massachusetts*, 944 F.3d 9 (1st Cir. 2019), is similarly misplaced. *See* Mot. 4, 11, 16. In that case, the court rejected a claim that the Massachusetts minimum wage statute was preempted by Department of State au pair regulations after holding that the "regulatory text that appears to point directly against" the reading the plaintiffs gave to the au pair regulations. *Capron*, 944 F.3d at 13-14, 42. Here, by contrast, the Attorney General points to nothing in the regulatory text suggesting that Congress or NHTSA welcomed an open-access vehicle systems regime and the cybersecurity threats it occasions. The court also noted that the Department of State previously took the opposite position on the conflict—that the au pair regulations do not preempt states from enforcing minimum-wage laws on those who employ au pairs. *Id.* at 43. Here, again, there is no such evidence.[6]

Nor does the fact that Plaintiff seeks facial relief on its preemption claims warrant dismissal. *Contra* Mot. 5-6, 12 n.8 (citing *Cal. Coastal Comm'n v. Granite Rock Co.*, 480 U.S. 572, 580 (1987); *Pharm. Research & Mfts. of Am. v. Concannon*, 249 F.3d 66, 74-75, 78-79 (1st Cir. 2001), *aff'd* 538 U.S. 644 (2003)). Notably, *Concannon* was decided *after* significant fact

[6] The court also pointed out the "disjuncture" in the regulated entity under the two laws—the au pair regulations addressed "the obligations of sponsors" while the "state wage and hour measures focus[ed] on the obligations of the employers to the domestic workers whom they employ." *Capron*, 944 F.3d at 41. Here, the Data Law, Vehicle Safety Act, and federal motor vehicle safety standards all impose their obligations directly on auto manufacturers like Plaintiff's members.

development on a preliminary injunction motion, ultimately turning on dueling affidavits about the effects of the allegedly preemptory law. The court concluded that it "simply cannot say on this record that the Act conflicts" with the federal requirement because affidavits about the law's effect were "controverted by the affidavits of other qualified individuals." *Concannon*, 249 F.3d at 78.

Similarly, *Granite Rock* was decided *after* the plaintiff had filed a motion for summary judgment, at a time when both sides agreed that there were "no material facts in dispute." 480 U.S. at 577. There, the Supreme Court was persuaded to dispose of the preemption claim because "[i]n the present posture of this litigation, the [defendant's] identification of a possible set of permit conditions not pre-empted by federal law is sufficient to rebuff [the plaintiff's] facial challenge to the permit requirement." *Id.* at 589. Here, by contrast, there are significant fact issues underlying the Vehicle Safety Act preemption claim that have yet to be developed at trial, as the Court has already noted. Further, the Attorney General has not even attempted to provide a limiting construction of the Data Law that would eliminate the statutory conflict alleged.

The Attorney General also makes no attempt to explain why a facial challenge is not especially appropriate here, given the implications for public safety raised in Plaintiff's claims. It would make no sense for Plaintiff or Plaintiff's members to wait until *after* manufacturers have weakened vehicle cybersecurity protections—in accordance with the Data Law but in conflict with the Vehicle Safety Act—before bringing suit. There is no requirement that plaintiffs must wait for predictable deleterious effects to take place before challenging a law. Pre-enforcement suits are commonplace. Indeed, the U.S. Supreme Court granted relief in a major pre-enforcement challenge just last Term. *See generally June Med. Servs. LLC v. Russo*, 140 S. Ct. 2103 (2020).

Moreover, contrary to the Attorney General's view (Mot. at 4), there is no special burden imposed on plaintiffs asserting a preemption claim under the Vehicle Safety Act. The Supreme

Court has conclusively held that preemption claims based on that Act are to be considered under "ordinary pre-emption principles," with the Act imposing no "special burden" on a preemption claim. *Geier*, 529 U.S. at 870; *see also, e.g.*, *id.* at 888 (Stevens, J., dissenting) (taking issue with the majority's "rejection of the presumption against pre-emption").

Finally, even if any presumption against preemption were somehow applicable to the Data Law challenge (it is not), the Complaint still states a claim sufficient to survive a Rule 12(b)(6) motion. After all, at the heart of conflict preemption is the precise scenario in which Plaintiff's members now find themselves—where it is "impossible for a private party to comply with both state and federal requirements." *English*, 496 U.S. at 79. The Complaint plausibly alleges that manufacturers have installed access controls to protect key vehicle functions, in accordance with the purpose and objectives of the federal Vehicle Safety Act—the very controls which they would be required to remove to satisfy the Data Law's open-access regime. Compl. ¶¶ 31-36, 57-58, 71-72.

B. It is Impossible for Automakers to Simultaneously Comply with the Data Law and the Vehicle Safety Act's "Make Inoperative" Prohibition.

The Data Act is conflict preempted for another, independent reason. The Vehicle Safety Act requires auto manufacturers not to remove or otherwise degrade their vehicles' critical safety features. *See* 49 U.S.C. § 30122(b). A "manufacturer . . . may not knowingly make inoperative any part of a device or element of design installed on or in a motor vehicle or motor vehicle equipment in compliance with an applicable motor vehicle safety standard prescribed under this chapter." *Id.* As alleged in the Complaint, Plaintiff's members have installed cybersecurity protections to prevent unauthorized access to vehicle systems that control regulated vehicle functions. Compl. ¶¶ 31-36. Those controls are a key "part" of the "device or element of design" that allows vehicles to comply with federal motor vehicle safety standards. 49 U.S.C. § 30122(b).

The Attorney General reaches a contrary conclusion about Section 30122(b) only by ignoring its plain text. Section 30122(b) does not apply only to elements of design specifically called out as required in a motor vehicle safety standard. *Contra* Mot. 12-13. By its plain terms, the statute applies to "*any* . . . element of design" that the manufacturer "installed on or in a motor vehicle or motor vehicle" to comply with a safety standard. Manufacturers protect core vehicle functions like acceleration and braking with a cybersecurity design element to ensure that they maintain compliance with safety standards. Compl. ¶ 106.

To support its atextual, narrow reading of Section 30122, the Attorney General cites (at 13) just one authority, *Clarke v. TRW, Inc.*, 921 F. Supp. 927, 935 (N.D.N.Y. 1996). But *Clarke* does not purport to address preemption. And in any event, it is inapplicable even on the Attorney General's telling: a "'plaintiff fails to state [a] claim for violation of § 30122 unless the motor vehicle safety standard[s]' are involved." Mot. 13 (quoting *Clarke*, 921 F. Supp. at 935) (internal citations omitted). Here, Plaintiff's challenge involves *several* motor vehicle safety standards.

As the Complaint alleges, NHTSA's federal motor vehicle safety standards are directly at issue here. *See* Compl. ¶¶ 102-03 (discussing FMVSS for acceleration controls systems, braking systems, and electronic stability control systems); *id.* ¶ 106 ("Auto Innovators' members have installed components to comply with various FMVSSs (*e.g.*, air bags, braking systems, steering systems, accelerator controls), nearly all of which are now controlled electronically, and for which members have installed safeguards to prevent electronic intrusion as part of their designs."); *contra* Mot. 8 (incorrectly asserting that Plaintiff "never identifies which federal vehicle safety regulations it claims to be preemptive").

Take, for instance, acceleration. FMVSS 124 regulates acceleration control devices. *See* 49 C.F.R. § 571.124. That standard presupposes that the driver will be in control of a vehicle's

acceleration. For example, it describes the feature it covers as a "[d]river-operated accelerator control system" and "establishes the requirements for the return of a vehicle's throttle to the idle position when *the driver* removes the actuating force from the accelerator control." *Id.* (emphasis added). By its text, the standard encompasses nearly anything related to how the accelerator functions - "all vehicle components, except the fuel metering device, that regulate engine speed in direct response to movement of the driver-operated control and that return the throttle to the idle position upon release of the actuating force." *Id.*

The same is true for braking. The FMVSS for light vehicle brake systems has the broad purpose of insuring "safe braking performance under normal and emergency conditions." 49 C.F.R. § 571.135 (FMVSS 135). That necessarily presupposes that the driver—not some third-party hacker—remains in control of braking. *See, e.g., id.* (stating that any brake power assist unit must ensure that while "reduc[ing] the amount of muscular force that *a driver must apply* to actuate the system" it "does not prevent *the driver from braking* the vehicle by a continued application of muscular force"); *id.* (discussing a brake power unit as involving the "*driver action* . . . of modulating the energy application level"); *id.* (discussing brake testing conditions to include "[p]edal force . . . *applied and controlled by the vehicle driver*) (emphases added).

Likewise, this applies to steering and anti-lock braking systems. Electronic stability control (ESC) systems are "computer-controlled with the computer using a closed-loop algorithm to limit vehicle oversteer and to limit vehicle understeer." 49 C.F.R. § 571.126 (FMVSS 126). The safe and approved operation of these systems relies on manufacturers to ensure that electronic inputs come from the driver, and that the driver remain in control. *See, e.g., id.* (describing the approved system as a "means to monitor *driver* steering inputs"); *id.* (requiring the "algorithm to determine the need, and a means to modify engine torque, as necessary, to *assist the driver in*

maintaining control of the vehicle"); *id.* (discussing the driver's ability "disable[] the ESC" system) (emphases added).

In an era in which vital vehicle functions like acceleration and braking are now controlled electronically, manufacturers have a statutory obligation to maintain design elements to ensure that regulated vehicle features continue to meet minimum safety requirements. A key part of doing so is the access controls that manufacturers maintain in their vehicles to ensure that those functions are not compromised by third parties. Compl. ¶¶ 19, 106. Although the particular cybersecurity features that Plaintiff's members may use to ensure the integrity of these electronically controlled vehicle functions may be up to members' discretion, *see* Mot. 7 (discussing NHTSA cybersecurity guidance), members cannot scuttle cybersecurity measures that protect driver-controlled devices from external threats. *Id.* ¶ 106.

This is not, as the Attorney General suggests, "speculation about future impacts supplied by the plaintiffs themselves." Mot. 11 (quoting *Capron*, 944 F.3d at 40). NHTSA called out these specific core vehicle functions as open to intrusion because of the Data Law's requirement that manufacturers *weaken* access controls around vehicle systems. Its primary concern was that this required weakening would invite cyberhacking that could compromise core vehicle functions like acceleration, braking, and steering. *See* Compl. Ex. A at 3, 4; Compl. ¶¶ 31, 74.

Nor are concerns of members and NHTSA "hypothetical," as the Attorney General claims. Mot. 11 (quoting *Rice v. Norman Williams Co.*, 458 U.S. 654, 659 (1982), for the proposition that "hypothetical or potential conflict is insufficient" for preemption). Manufacturers spend significant labor hours and money keeping access controls up to date to prevent cyberhackers from penetrating their vehicle systems. Compl. ¶ 34. Plaintiff details in its Complaint the recent rise in cyberhacking attempts. *Id.* ¶¶ 19, 175 (discussing FBI reports); *see also id.* ¶¶ 73-74 (discussing

Chrysler cybersecurity-related recall). As discussed in media reports at that time of the Chrysler recall, security researchers using the Internet were able to "infiltrate a Jeep Cherokee's electronics systems and hijack many of the vehicle's features, all while the duo sat in a basement miles from where [a reporter] was driving the SUV." PBS, *Fiat Chrysler announces recall after hackers gain control of moving car* (July 25, 2015), https://www.pbs.org/newshour/nation/fiat-chrysler-announces-recall-response-hackers-gaining-control-moving-car. Among other things, the hackers "disable[d] [the vehicle's] transmission," and "cripple[d] its brakes and control[led] its steering." *Id.*

The Attorney General's reading of Section 30122(b) would lead to absurd results. Take, for instance, FMVSS 208, which concerns airbags. Manufacturers are required to design airbags to meet that standard's explicit performance criteria. *See* 49 C.F.R. § 571.208. But manufacturers also have an obligation to design airbags to ensure that they function as airbags are supposed to—that is, that they do not explode metal shrapnel when they deploy, or fail because of exposure to high humidity, or deploy uncommanded—even though none of those three things is required by explicit text in FMVSS 208. *See id.* To take steps that would make those results more likely would compromise the most basic element of design of an airbag covered by the safety standards promulgated under the Vehicle Safety Act. Likewise, NHTSA expects that manufacturers will provide appropriate cyber protections around vehicle features like airbags to prevent unwanted intrusion by hackers who could wreak mischief with remote deployment commands. Yet under the Attorney General's non-sensical reading of the Vehicle Safety Act and regulations, NHTSA would somehow be foreclosed from taking action against manufacturers that compromised the core essential function of that vehicle feature.

As evidenced by the Chrysler recall, NHTSA does not understand its Section 30122 regulatory authority to be so narrow. *See* pp. 8-9, *supra*. Just this past month, NHTSA proposed a rule that would add an additional exemption to Section 30122(b)'s "make inoperative" provision. *See* 85 Fed. Reg. 84281 (Dec. 28, 2020). The proposed exemption would allow the installation of rear-mounted transporters to vehicles to improve mobility for drivers and passengers with disabilities even though the installation of those devices could block a backup camera's view. *Id.* Backup cameras are contemplated in FMVSS 111, regulating rearview image. *See* 49 C.F.R. § 571.111. But although that FMVSS discusses a vehicle's rear viewing range, including with a backup camera, it makes no explicit mention of a prohibition on devices that would obstruct a portion of that range. *Id.* Nonetheless, NHTSA felt it necessary to propose a rule exempting rear-mounted transponders from Section 30122(b) liability for rendering backup cameras partially inoperative, reinforcing that the Attorney General's proposed narrow interpretation of the Vehicle Safety Act is incorrect as a matter of law.

II. Plaintiff Has Stated a Plausible Preemption Claim Under the Clean Air Act.

For similar reasons, Plaintiff has stated a plausible conflict preemption claim under the Clean Air Act. Compl. ¶¶ 107-115. Plaintiff's members cannot "comply with both state and federal requirements," and the Data Law "stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress" in the Act. *Oneok, Inc. v. Learjet, Inc.*, 575 U.S. 373, 377 (2015). As alleged in the Complaint, the Data Law would force members, in violation of federal law, "to remove or render inoperative" access controls manufacturers have in place to prevent tampering with their vehicle emissions systems. 42 U.S.C. § 7522(a)(3)(A). Without those access controls in place, owners (or third parties) would have the easy ability to modify vehicle emissions through such mechanisms as aftermarket defeat devices. *See* Compl. ¶¶ 52, 114-15.

The Attorney General spends several pages arguing that the Data Law does not attempt to establish a "standard" of vehicle emissions, *see* Mot. 13-14, which indeed the law does not. Although the drafters of the Data Law likely did not intend to weaken compliance with federal emissions requirements in Massachusetts vehicles, that is the inevitable effect of the Data Law's requirement that manufacturers relinquish control of access to their vehicle systems, including those protecting emissions. *See* Compl. ¶¶ 52, 114-15.[7]

As with the Vehicle Safety Act, the Attorney General's motion is premised on a reading of the Clean Air Act at odds with the statutory text. *See* Mot. 15. The relevant provision prohibits, in full, "any person to remove or render inoperative *any* device or *element of design* installed on or in a motor vehicle or motor vehicle engine in compliance with regulations under this subchapter prior to its sale and delivery to the ultimate purchaser, or for any person knowingly to remove or render inoperative any such device or element of design after such sale and delivery to the ultimate purchaser." 42 U.S.C. § 7522(a)(3)(A) (emphasis added). As with the Vehicle Safety Act, then, the statute sweeps broadly to encompass "any" element of design. *Id.* Further, the "element of design" need not itself be explicitly required by applicable regulations, but merely one "installed . . . in compliance with regulations." *Id.*

EPA regulations take a broad view of design elements. Among other things, the definition of an "[e]lement of design" includes "any control system (*i.e.*, computer, software, electronic control system, emission control system, computer logic)" in the vehicle. 40 CFR § 86.1803-01.

[7] The Attorney General's own authority (Mot. 14) provides that "standard" encompasses any "emission characteristics of a vehicle or engine," including "not only 'numerical emission levels with which vehicles or engines must comply,' but also [the] 'emission-control technology with which they must be equipped." *In re Volkswagen "Clean Diesel" Mktg., Sales Practices, and Prods. Liab. Litig.*, 959 F.3d 1201, 1216-18 (9th Cir. 2020) (quoting *Engine Mfrs. Ass'n v. S. Coast Air Quality Mgmt. Dist.*, 541 U.S. 246, 252-53 (2004)). Here, Plaintiff alleges that the removal of access controls required by the Data Law will hinder vehicle emission-control technology. *See* Compl. ¶ 115.

Consistent with that regulatory definition, as an element of design, Plaintiff's' members maintain rigorous access controls around vehicle systems to ensure against unauthorized access that could impact emissions. *See* Compl. ¶ 115.

Contrary to the Attorney General's assertion, *see* Mot. 15, several federal regulations are directly implicated by the Data Law's weakening of access controls around vehicle emission systems. The Clean Air Act imposes stringent vehicle-emissions requirements on manufacturers. For instance, manufacturers of new motor vehicles must warrant the emission control system of the vehicle for the "useful life" of the vehicle"—either 10 years or 100,000 miles. 42 U.S.C. §§ 7521(d), 7541(a)(1)). As part of that obligation, manufacturers must perform in-use verification testing on post-sale vehicles at regular mileage intervals prescribed by federal regulation. *See* 40 C.F.R. § 86.1845-04. And the EPA retains the right to require manufacturers to make changes to the configuration of vehicles, including changes to the vehicle's software, to ensure that vehicles continue to meet federal emissions-control limits. *See id.* § 86.1842-01(b). The Data Law's requirement that manufacturers abandon their current system of access controls in favor of an open-access regime will frustrate manufacturers' ability to satisfy their federal regulatory obligation to keep vehicles emissions compliant. Compl. ¶¶ 10, 52, 114-15.

It is irrelevant that the Data Law does not "require[] anyone to disable or tamper with an emissions-control device." Mot. 15. For similar reasons to those explained by NHTSA in the context of the Vehicle Safety Act, enabling such hacking is the predictable effect of a law that weakens access controls. This is not baseless "speculation." *Id.* at 16. As discussed above, the Data Law requires manufacturers to eliminate their existing access controls and provide open access to their vehicle systems to read and modify vehicle data, as well as write new data to those systems. SD645 § 3. As a result of those required changes, vehicle owners (or third parties) would

have ready access to a vehicle's engine control module to disable emissions control systems via after-market software designed for that purpose. *See* Compl. ¶¶ 114-15.

The Data Law thus impermissibly prevents auto manufacturers from ensuring that their vehicles remain compliant with current emissions standards by facilitating violations of the Clean Air Act by third parties utilizing defeat devices to manipulate vehicle performance and circumvent emissions controls. *See* Compl. ¶¶ 114-15. At the very least, Plaintiff should have a chance to prove facts in support of its claim before its allegations are cast aside as "speculation," particularly given that the Attorney General has failed to offer any explanation as to how it is supposedly possible for any manufacturer to comply with the Data Law without running afoul of the Clean Air Act and the regulations promulgated thereunder. The very cases on which the Attorney General relies (Mot. at 16) to argue for dismissal of a pre-enforcement challenge—*Capron* and *Concannon*—were decided only *after* the very factual development that the Attorney General's motion seeks to prevent here. *See* pp. 10-11, *supra*.

III. Counts 3 Through 7 Should Be Stayed, But Also Survive Rule 12(b)(6)

Because Plaintiff has moved to stay Counts 3 to 7 of the Complaint pending the outcome of the expedited trial on the merits (ECF 57), there is no need to address those counts now. But even if ripe for consideration, the Attorney General's motion to dismiss those counts also fails, as each plausibly alleges a valid claim.

A. Plaintiff's Takings Claim Is Not Foreclosed by Law.

The Attorney General does not dispute that Plaintiff alleges a viable takings claim. Indeed, the Attorney General never so much as addresses the two takings theories—physical and regulatory—on which Plaintiff relies in its Complaint. Compl. ¶¶ 163-70. Instead, the Attorney General focuses her argument entirely on the procedure by which Plaintiff seeks to redress the Data Law's uncompensated taking. Citing *Knick v. Township of Scott*, 139 S. Ct. 2162 (2019), the

Attorney General claims that Plaintiff cannot seek declaratory relief in federal court because Massachusetts allows for an inverse-condemnation action. Mot. 24-26.

Contrary to the Attorney General's assertions, *Knick* compels the denial of the motion to dismiss. *Knick* expressly overruled the very state-remedy exhaustion requirement the Attorney General seeks to impose here, and holds that the constitution "guarantees a federal forum for takings plaintiffs." 139 S. Ct. at 2167, 279 (overturning in part *Williamson Cnty. Reg. Planning Comm'n v. Hamilton Bank of Johnson City*, 473 U.S. 172 (1985)). As the Supreme Court recognized, the existence of a state-law remedy "cannot infringe or restrict the property owner's federal constitutional claim" without impermissibly "handing authority over federal takings claims to state courts." *Knick*, 139 S. Ct. at 2169-71.

In conflict with that very holding, the Attorney General seeks to elevate into a new, broad-ranging constitutional rule the *Knick* court's observation, in dicta, that "the availability of post-taking compensation" in federal court will "ordinarily" render injunctive relief unnecessary. *Id.* at 2177; *see* Mot. 24-25. But Plaintiff here seeks only declaratory relief. Moreover, *Knick* involved a takings claim against a municipality, from which the plaintiff unquestionably could seek compensation. 139 S. Ct. at 2177 (discussing "[t]akings claims against local governments"). The takings claim here is against a state. As the Attorney General is quick to point out, a claim seeking monetary compensation from the Commonwealth in federal court is foreclosed by the Eleventh Amendment. Mot. 25-26; *see, e.g.*, *Seven Up Pete Venture v. Schweitzer*, 523 F.3d 948, 956 (9th Cir. 2008) ("[T]he Eleventh Amendment bars reverse condemnation actions brought in federal court against state officials in their official capacities."). Thus, lest "the guarantee of a federal forum ring[] hollow for takings plaintiffs," *Knick*, 139 S. Ct. at 2167, Plaintiff must seek equitable relief to remedy the wrongs in the Data Law. *See, e.g.*, *Fowler v. Guerin*, 899 F.3d 1112, 1120

(9th Cir. 2018) (allowing takings claim seeking injunctive relief); *accord Ex parte Young*, 209 U.S. 123, 159-60 (1908)).

Moreover, particularly given the *Knick* court's explicit overruling of *Williamson*, there is no occasion to read *Knick* as overruling *sub silentio* the Supreme Court's many prior cases approving equitable takings relief. *See, e.g.*, *Babbit v. Youpee*, 519 U.S. 234, 242-43 (1997) (holding declaratory and injunctive relief appropriate in an action challenging the constitutionality of a federal statute providing for the escheat of fractional interests in land); *Eastern Enters. v. Apfel*, 524 U.S. 498, 538 (1988) (plurality op.). Indeed, courts have continued to allow takings plaintiffs to seek such relief in the wake of *Knick*. *See, e.g.*, *Cmty. Hous. Improvement Prgm. v. City of New York*, Nos. 19-cv-4087, -6447, 2020 WL 5819900, at *5 (E.D.N.Y. Sept. 30, 2020) ("[p]laintiffs may continue to seek prospective remedies—like an injunction—against state officials under *Ex Parte Young*").

Although there is no need to go further, the Attorney General's argument also fails because it is premised on the erroneous assumption that the Data Law constitutes a valid taking. The state court inverse condemnation proceeding suggested by the Attorney General (Mot. 24 n.9) necessarily presupposes a proper taking. It allows claimants "to secure compensation in the event of *otherwise proper* interference amounting to a taking." *First English Evangelical Lutheran Ch. of Glendale v. L.A. Cnty.*, 482 U.S. 304, 315 (1987) (emphases altered). Thus, courts generally recognize that plaintiffs "may not plead inverse condemnation in good faith without being prepared to accept just compensation in exchange for [their] property." *Race v. Bd. of Comm'rs of the Cnty. of Lake, Colo.*, 2017 WL 3334647, at *9 (D. Colo. Aug. 4, 2017). But Plaintiff has alleged that the Data Law is improper for a host of constitutional reasons—including that it is preempted under several federal statutes and will occasion substantial public harm at manufactures' expense to

deliver a private benefit to politically favored actors. In those circumstances, inverse-condemnation relief is inadequate. *See, e.g., Int'l Union of Operating Engineers Local 0139 v. Schimel*, 863 F.3d 674, 678 n.2 (7th Cir. 2017) ("[I]t is well accepted that, when the government has taken property for a private . . . use, injunctive or declaratory relief may be appropriate."). This is particularly true here, given the substantial unquantifiable reputational costs for manufacturers as a result of a serious data breach occasioned by the Data Law's open-access requirements. Compl. ¶¶ 15, 170; *cf. Duke Power Co. v. Carolina Envt'l Study Grp., Inc.*, 438 U.S. 59, 71 n.15 (1978) (holding that equitable relief is appropriate when the government action would produce "potentially uncompensable damages").

Finally, Plaintiff here seeks only declaratory relief, and does not seek an injunction on its takings claim. As the Supreme Court has long observed, "different considerations enter into a federal court's decision as to declaratory relief, on the one hand, and injunctive relief, on the other." *Steffel v. Thompson*, 415 U.S. 452, 469 (1974). A declaration that a law is invalid is "a much milder form of relief than an injunction." *Id.* at 471.

B. Plaintiff's Intellectual Property Claims Should Not Be Dismissed.

1. Plaintiff Has Stated a Plausible Preemption Claim Under the Copyright Act.

Count 3 of the Complaint alleges that the Data Law is preempted by the Copyright Act, 17 U.S.C. § 101, because the Data Law's "open access" regime eliminates manufacturers' rights to exclude unauthorized users from accessing its copyrighted systems and the copyrighted works contained on them. Compl. ¶¶ 116-128. The Attorney General does not dispute that the Copyright Act provides broad federal protection for intellectual property rights which states are not free to modify. *See* 17 U.S.C. § 106(1)-(3), § 301(a). Nor does she dispute that Plaintiff's members' vehicle systems are protected under the Copyright Act because they include original and creative elements. *See id.* § 102(a); *see also* Compl. ¶¶ 78-82, 121.

Instead, the Attorney General argues that because the Data Law targets "access to data," there is no reason to believe that the copyrighted features on members' vehicle systems will be accessible. Mot. 19. That is an implausible interpretation of a law that by its terms requires manufacturers to abandon control over who has access to their systems. SD645 §§ 2, 3. There is no existing way for manufacturers to confine hackers' access only to data, once their ability to enforce their current systems of access controls is nullified. *E.g.*, Compl. ¶¶ 9, 10, 12, 20, 43.

The Attorney General acknowledges (Mot. 19) that Plaintiff alleged a classic copyright violation that would be occasioned by the Data Law—when an unauthorized user accessing a vehicle system to read or write data creates a new fixed copy in the computer's random access memory. *See* Compl. ¶ 124. Yet, the Attorney General claims that such copying is somehow irrelevant because of where the copy ultimately may reside. *See* Mot. 19. The law does not support this distinction. The Copyright Act prohibits any unauthorized copy that will result from that access, regsardless of where that copy will reside. *See, e.g.*, *Cartoon Network LP v. CSC Holdings, Inc.*, 536 F.3d 121, 130 (2d Cir. 2008) (cable subscriber infringed copyright when the subscriber caused a television program to be copied in the server's memory); *MAI Sys. Corp. v. Peak Computer, Inc.*, 991 F. 2d 511, 518 (9th Cir. 1993) (party infringed copyright by causing copies to be made on systems belonging to third parties).

The Attorney General also claims that any infringement occasioned by the Data Law would be "fair use," but makes no attempt to explain why or even address the statutory fair-use factors. *See* Mot. 19.[8] Plaintiff's members alleged that they have spent billions of dollars creating secure vehicle systems, over which they maintain strict access control to protect those systems. *See*

[8] The factors are (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work. *See* 17 U.S.C. § 107.

Compl. ¶¶ 28-36, 77, 168. By removing manufacturers from the process of determining who can access their systems (and what users can do on those systems after accessing them), the Data Law sweeps well beyond any incidental fair use. Moreover, the fair use factors are fact-dependent and generally cannot be resolved on a motion to dismiss. *See, e.g.*, *Browne v. McCain*, 611 F. Supp. 2d 1073, 1078 (C.D. Cal. 2009) ("[C]ourts rarely analyze fair use on a 12(b)(6) motion").

Finally, the Attorney General claims in passing that Plaintiff lacks standing to "seek an injunction for copyright infringement," asserting that only its members can do so. Mot. 19 (quotation omitted). That is incorrect. For one, Plaintiff is not seeking an injunction for copyright infringement. Its claim is premised on the Supremacy Clause and the conflict between the open-access requirements in the Data Law and federal law that protects members' rights to exclude. Compl. ¶¶ 116-28. The Attorney General's lone authority—*Authors Guild, Inc. v. HathiTrust*, 755 F.3d 87, 94 (2d Cir. 2014)—concerned only infringement claims, and thus is inapplicable.

In any event, each of Plaintiff's members is without question "[t]he legal or beneficial owner of an exclusive right under a copyright," and thus is entitled to "institute an action" to assert that right. 17 U.S.C. § 501(b). Plaintiff is seeking relief on their behalf pursuant to well-settled notions of associational standing. *See* Part IV, *infra*. That standing does not expand the class entitled to sue; it merely permits an association to bring claims "solely as the representative of its members" who have standing to sue in their own right. *Warth v. Seldin*, 422 U.S. 490, 511 (1975).[9]

[9] Courts routinely allow associations to assert statutory rights in similar circumstances. In *Southern Illinois Carpenters Welfare Fund v. Carpenters Welfare Fund of Illinois*, for instance, the court held that unions have standing to assert ERISA claims on behalf of members despite the statute "confin[ing] the right to sue . . . to plan participants" because that limitation did not evince that "Congress intended to prevent unions from suing on behalf of participants." 326 F.3d 919, 922 (7th Cir. 2003). The "union in such a case is not seeking anything for itself; the real plaintiffs in interest are [its] plan participant" members. *Id.*

2. Plaintiff Has Stated a Plausible Preemption Claim Under the CFAA.

Count 5 of the Complaint alleges that the Data Law is preempted by the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, because the "open access" platforms it requires would eliminate manufacturers' rights to determine who is an authorized user or for what purpose third parties may use their vehicle systems. Compl. ¶¶ 139-47. That would conflict with the CFAA's purpose—preventing users from "'obtaining . . . information from any protected computer." "without authorization." 18 U.S.C. § 1030(a)(2)).

The Attorney General does not dispute that members' vehicle systems are "protected computers" under the CFAA, Compl. ¶ 145 (citing 18 U.S.C. § 1030(e)(1)), or deny that third parties "obtain[] . . . information" from manufacturers' vehicle systems when they access those systems, *see id.* ¶¶ 91, 145-46. Instead, citing one case—*CDK Global LLC v. Brnovich*, 461 F. Supp. 3d 906, 915-16 (D. Ariz. 2020), currently up on appeal, *see* No. 20-16469 (9th Cir.)—the Attorney General claims that the CFAA leaves the scope of authorization to state law, meaning Massachusetts can grant vehicle owners the right to authorize access to vehicle systems owned and operated by manufacturers. Mot. 21-22. That is wrong. The CFAA gives *owners* "exclusive discretion" to determine who can access their systems. *United States v. Nosal*, 844 F.3d 1024, 1036 (9th Cir. 2016); *accord, e.g.*, *In re Dealer Mgmt. Sys. Antitrust Litig.*, 362 F. Supp. 3d 558, 570 (N.D. Ill. 2019) ("the 'authorization' required for lawful access under the CFAA must come from the owner of the computer system"); *Christie v. Nat'l Inst. for Newman Studies*, 2019 WL 1916204, at *7 (D.N.J. Apr. 30, 2019) (same); *Univ. Sports Pub. Co. v. Playmakers Media Co.*, 725 F. Supp. 2d 378, 384 (S.D.N.Y. 2010) (holding that "the term 'exceeds authorized access'" as used in the CFAA "applies to authorized users who cross boundaries set by the system owner").

Again relying on *CDK*, the Attorney General claims that the CFAA is aimed at punishing and deterring high-tech hacker crimes, not preempting state statutes that expand access. Mot. 21-

22. But this case *is* about deterring high-tech hacker crimes. *See* Compl. ¶¶ 19, 175. In any case, the Attorney General's argument rests yet again on an overly narrow conception of preemption. Congress need not express its intent to preempt state laws for conflict preemption to apply. The CFAA "prohibits acts of computer trespass by those who are not authorized users or who exceed authorized use"—full stop. *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1065 (9th Cir. 2016). Because the Data Law purports to override this prohibition, it "stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress." *Hines*, 312 U.S. at 67; *accord, e.g., Crosby v. Nat'l Foreign Trade Council*, 530 U.S. 363, 373 (2000).

3. Plaintiff Has Stated a Plausible Preemption Claim Under the DMCA.

Count 6 of the Complaint alleges that the Data Law is preempted by the Digital Millennium Copyright Act, 17 U.S.C. § 1201, because its "open access" regime compels manufacturers to abandon the access controls they have in place to control access to their vehicle systems. Compl. ¶¶ 148-59. The DMCA express Congress's desire to prevent the "circumvention[]" of "a technological measure that effectively controls access to a [copyrighted] work." 17 U.S.C. § 1201(a)(1)(A). The Attorney General does not dispute that Auto Innovators' members use technological measures to effectively control access to the copyrighted works residing in their vehicle systems, *see* Compl. ¶¶ 33, 157—measures they alleged that they would have to abandon to comply with the Data Law's "open access" requirements and quick timeframe, *see id.* ¶159.

Instead, echoing its CFAA arguments, the Attorney General contends that Massachusetts is free to give whomever it chooses the authority to authorize access on manufacturers' behalf. Mot. 23-24.[10] But Congress's intent in enacting the DMCA was to deter digital copyright

[10] Yet again, the Attorney General relies (Mot. 23) almost entirely on *CDK*, which interpreted the DMCA in the altogether different context of a state law that required providing access to data consistently mostly of information not protected by copyright. *CDK*, 461 F. Supp. 3d at 916. And nothing in the Attorney General's other case—*Ground Zero Museum Workshop v. Wilson*, 813 F. Supp. 2d 678 (D. Md. 2011)—

infringement by amplifying "*the copyright owner's* right to control access to his or her copyrighted work." H.R. Rep. No. 105-551, pt. 2, at 38 (1998) (emphasis added). Thus, unlawful "'circumvent[ion]'" of "'a technological measure'" is defined to mean "to avoid, bypass, remove, deactivate, or impair a technological measure, *without the authority of the copyright owner*." 17 U.S.C. § 1201(a)(3)(A) (emphasis added). Recognizing that copyright owners need "reasonable assurance that they will be protected against massive piracy" in order to make their works available in a digital environment, Congress enacted the DMCA to "encourage[]" owners' adoption of "technological solutions" to control access. S. Rep. No. 105-190 at 8, 11 (1998). The new Data Law cannot be reconciled with that provision either.

4. Plaintiff Has Stated a Plausible Preemption Claim Under the DTSA.

Count 4 of the Complaint alleges that the Data Law is preempted by the Defend Trade Secrets Act ("DTSA"), 18 U.S.C. § 1386, because it impossible for manufacturers to provide the required "open access" platforms without leaving vulnerable the manufacturers' proprietary trade secrets which are protected by the federal DTSA. Compl. ¶¶ 129-38. The Attorney General argues that this claim fails as a matter of law because the challenged statute, as codified in Chapter 93K, contains an exception stating that "nothing in this chapter shall be construed to require a manufacturer to divulge a trade secret." M.G.L. c. 93K, § 3 (2013). According to the Attorney General, this language eliminates any possibility of a statutory conflict. Mot. 20-21.

The Attorney General's argument fails on the current record. Plaintiff has adequately alleged that it is not possible for manufacturers to comply with the new law without jeopardizing their trade secrets. Compl. ¶¶ 137-38. Although Chapter 93K, Section 3 provides that nothing

---

suggests that anyone other than the copyright owner may control access to copyrighted material. Rather, the court dismissed a DMCA liability claim because plaintiffs had "not alleged any facts to suggest that [the defendant] ever accessed the [plaintiff's] website without using a security pass code issued by Plaintiffs or [their agent]." *Id.* at 692.

elsewhere in the statute requires manufacturers to divulge their trade secrets, the Attorney General has not issued a notice or otherwise clarified that Sections 2 and 3 of the new law are therefore unenforceable against manufacturers. Without that clarification, manufacturers are left with the impermissible "choice" of risking their trade secrets to comply with the new law (which is prohibited by the DTSA), or not complying with the new law, and then having the Attorney General claim that the open access provisions of the statute somehow remain enforceable notwithstanding the statutory trade secret exception.

IV. Plaintiff Has Established Associational Standing.

"An association has standing to sue on behalf of its members [if]: (1) at least one of the members possesses standing to sue in his or her own right; (2) the interests that the suit seeks to vindicate are pertinent to the objectives for which the organization was formed; and (3) neither the claim asserted nor the relief demanded necessitates the personal participation of affected individuals." *United States v. AVX Corp*, 962 F.2d 108, 116 (1st Cir. 1992) (discussing *Hunt v. Wash. State Apple Adver. Comm.*, 432 U.S. 333, 343 (1977)).

Here, the Attorney General concedes that Plaintiff has satisfied the first two *Hunt* factors, and therefore that the constitutional requirements for associational standing have been met. Mot. 27. The Attorney General instead seeks dismissal pursuant to Rule 12(b)(1) based on the third *Hunt* prong, which is purely prudential. The Attorney General asserts that a trial of the facts will "require participation by [Plaintiff's] individual members," and speculates that factual "differences" between members and how their proprietary vehicle systems operate may prove "salient." Mot. 28. But Plaintiff has already submitted affidavits from *twenty* separate members in support of its motion for preliminary injunction (*see* ECF Nos. 29-48), and the Attorney General tellingly fails to identify even one salient factual distinction between those members' vehicle systems that bears on the preemption analysis. Further, the Court has already established a

mechanism to ensure that Plaintiff identifies, early in the case, a limited number of member fact witnesses Plaintiff intends to call at trial, and to allow the Attorney General to take discovery from those members.

As the First Circuit has recognized, "just because a claim may require proof specific to individual members of an association does not mean the members are required to participate as parties in the lawsuit." *Pharm. Care Mgmt. Ass'n v. Rowe*, 429 F.3d 294, 306 (1st Cir. 2005). Where the plaintiff association's claim turns largely on expert evidence, the participation of plaintiff's individual members as parties is not necessary to litigate the action. *Camel Hair & Cashmere Inst. of Am., Inc. v. Associated Dry Goods Corp.*, 799 F.2d 6, 12 (1st Cir. 1986). Even if the inquiry is "fact specific" and the associational plaintiff will be required to "introduce proof of specific [member] practices and effects," the members need not participate as parties, particularly given that, as here, the remedy sought would "inure to the benefit" of all the members. *Rowe*, 429 F.3d at 306. Actions for declaratory, injunctive, and other forms of prospective relief are particularly suited to group representation. *Students for Fair Admissions, Inc. v. President & Fellows of Harvard Coll.*, 261 F. Supp. 3d 99, 110 (D. Mass. 2017), *aff'd sub nom. Students for Fair Admissions, Inc. v. President & Fellows of Harvard Coll.*, 980 F.3d 157 (1st Cir. 2020).[11]

CONCLUSION

For the foregoing reasons, the Attorney General's motion to dismiss should be DENIED.

Dated: January 8, 2021

[11] The Attorney General's reliance on *National Ass'n of Government Employees v. Mulligan*, 914 F. Supp. 2d 10 (D. Mass. 2012) is misplaced. There, the relief sought by the association undisputedly "pit[ted] the interests of one faction of its membership against the interests of another faction." *Id.* at 12. The Attorney General does not and cannot demonstrate the existence of any such competing factions here.

Respectfully submitted,

ALLIANCE FOR AUTOMOTIVE INNOVATION

By its attorneys,

/s/ Laurence A. Schoen

Laurence A. Schoen, BBO # 633002
Elissa Flynn-Poppey, BBO# 647189
Andrew N. Nathanson, BBO#548684
MINTZ, LEVIN, COHN, FERRIS,
GLOVSKY, AND POPEO, P.C.
One Financial Center
Boston, MA 02111
Tel: (617) 542-6000
lschoen@mintz.com
eflynn-poppey@mintz.com
annathanson@mintz.com

John Nadolenco (*pro hac vice*)
Andrew J. Pincus (*pro hac vice*)
Erika Z. Jones (*pro hac vice*)
Archis A. Parasharami (*pro hac vice*)
Eric A. White (*pro hac vice*)
MAYER BROWN LLP
1999 K Street, NW
Washington, DC 20006
Tel: (202) 263-3000
jnadolenco@mayerbrown.com
apincus@mayerbrown.com
ejones@mayerbrown.com
aparasharami@mayerbrown.com
eawhite@mayerbrown.com

Charles H. Haake (*pro hac vice*)
Jessica L. Simmons (*pro hac vice*)
ALLIANCE FOR AUTOMOTIVE INNOVATION
1050 K Street, NW
Suite 650
Washington, DC 20001
Tel: (202) 326-5500
chaake@autosinnovate.org
jsimmons@autosinnovate.org

CERTIFICATE OF SERVICE

I hereby certify that this document, filed through the ECF system, will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF) and that paper copies will be sent to those indicated as non-registered participants on January 8, 2021.

/s/ Laurence A. Schoen
Laurence A. Schoen

106974117v1